CLAIMS

What is claimed is:

Sub a5

~~1. A method for providing a cryptographic service utilizing a server on a network, comprising:~~

~~(a) identifying a client utilizing the network;~~

~~(b) establishing a first key;~~

~~(c) generating a tunnel on the network;~~

~~(d) receiving information at the server from the client utilizing the tunnel, wherein the information is encrypted by the client using the first key; and~~

~~(e) performing work at the server.~~

~~2. A method as recited in claim 1, wherein a second key is encrypted by the client using the first key, and further comprising receiving the second key at the server.~~

~~3. A method as recited in claim 2, wherein the second key comprises at least one parameter for the work performed by the server.~~

~~4. A method as recited in claim 1, wherein the work includes cryptographic services.~~

~~5. A method as recited in claim 1, wherein the work includes modular exponentiation.~~

~~6. A method as recited in claim 1, further comprising the step of transmitting work results to the client.~~

~~7. A method as recited in claim 6, further comprising the step of encrypting the work results utilizing the first key.~~

8. A method as recited in claim 6, wherein the work results are transmitted to a third party.

A5

9. A method as recited in claim 1, further comprising the step of charging a fee for the work performed by the server.

10. A method as recited in claim 9, wherein the fee is charged to the client.

11. A method as recited in claim 1, wherein the first key comprises an encryption key for a symmetric cipher.

12. A method as recited in claim 1, wherein the first key comprises an encryption key for an asymmetric cipher.

13. A computer program embodied on a computer readable medium for providing a cryptographic service utilizing a server on a network, comprising:

(a) a code segment for identifying a client utilizing the network;

(b) a code segment for establishing a first key;

(c) a code segment for generating a tunnel on the network;

(d) a code segment for receiving information at the server from the client utilizing the tunnel, wherein the information is encrypted by the client using the first key; and

(e) a code segment for performing work at the server.

14. A computer program as recited in claim 13, wherein a second key is encrypted by the client using the first key, and further comprising a code segment for receiving the second key at the server.

15. A computer program as recited in claim 14, wherein the second key comprises at least one parameter for the work performed by the server.

16. A computer program as recited in claim 13, wherein the work includes cryptographic services.

A5

17. A computer program as recited in claim 13, wherein the work includes modular exponentiation.

18. A computer program as recited in claim 13, further comprising a code segment that transmits work results to the client.

19. A computer program as recited in claim 18, further comprising a code segment that encrypts the work results utilizing the first key.

20. A system for providing a cryptographic service utilizing a server on a network, comprising:

(a) logic for identifying a client utilizing the network;

(b) logic for establishing a first key;

(c) logic for generating a tunnel on the network;

(d) logic for receiving information at the server from the client utilizing the tunnel, wherein the information is encrypted by the client using the first key; and

(e) logic for performing work at the server.

21. A method as recited in claim 3, wherein a message or a cyphertext comprises a second parameter for the work performed by the server.

22. A method as recited in claim 21, wherein the message or cyphertext has been blinded by the user before transmittal to the server.